REMARKS

Applicant has made minor clarifying amendments to claims 2-5 and 10 to delete "victim" and clarify the recitation of data center. No new matter has been added and these amendments require only minimal consideration and no further search by the examiner, since they are directed to minor antecedent basis errors that were not previously recognized by applicant or the examiner. Entry of these amendments will place the application in condition for allowance and/or simplify issues on appeal.

The examiner maintained the rejection of Claims 1-12 and 15-33 under 35 U.S.C. 102(e) as being anticipated by Yavatkar et al., (Yavatkar) U.S. Patent No. 6,735,702.

The examiner maintains that Yavatkar teaches:

> **... sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors (col. 3 line 65 - col. 4, line 23); sending the statistical information from the data collectors in response to the queries (col. 3 line 65 - col. 4, line 23); processing the statistical information to determine the source of suspicious network traffic heir sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53, agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node).**

In dealing with this rejection, it may be more elucidating if applicant deals with the examiner's supplemental reasoning kindly given in the examiner's "Response to Arguments." The examiner distills Applicant's argument to "(A) Argument: Yavatkar does not teach that the bloodhound agents are responsive to queries for statistical information."

At the outset, this is an oversimplification of Applicant's argument where Applicant in fact argued that Yavatkar failed to describe or suggest: "sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors and processing the

statistical information to determine the source of suspicious network traffic sent to the data center and gave reasons therefore.

Applicant contends that the relevant features of claim 1 that are not shown by the reference include: sending queries to data collectors, data collectors that collect statistical information, and processing statistical information to determine the source of suspicious network traffic ... .

In the examiner's response, the examiner reminds applicant that the claims must be given their broadest reasonable interpretation and then proceeds to equate Applicant's feature of: "sending queries to data collectors..." to Yavatkar teachings of a "watchdog agent launching various types of bloodhound agents based on the type of attack detected ... ." The examiner then equates: "The gathered information" of Yavatkar "to the statistical information because the claim language merely recites statistical information and does not specify the type of statistical information that is collected."

In construing features of claim 1 such as "sending queries" as "launching bloodhound agents," or "collect statistical information on network packets sent over the network" to "gathered information" the Examiner ignores guidance from the Federal Circuit such as in *In re Morris*[1] which stands for the principle that while the Office is entitled to construe claim terms using their "broadest reasonable meaning," the Examiner must apply the Court's guidance on what "reasonable" means:

> Since it would be unreasonable for the PTO to ignore any interpretive guidance afforded by the applicant's written description, either phrasing connotes the same notion: as an initial matter, the PTO applies to the verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, *taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description* contained in the applicant's specification." [emphasis supplied]

According to *Morris,* the examiner must apply the broadest reasonable meaning "in their ordinary usage as they would be understood by one of ordinary skill in the art." The examiner

[1] *In re Morris*, 127 F.3d 1048 (Fed. Cir. 1997).

has not provided any rational basis upon which one of ordinary skill in the art would construe "sending queries to data collectors" as the same as launching bloodhound agents based on the type of attack detected or construing "statistical information on network packets" as "gathered information." For example, the examiner states: "The gathered information is equated to the statistical information because the claim language merely recites statistical information and does not specify the type of statistical information that is collected." Applicant contends that had Yavatkar described collecting statistical information on network traffic, then the examiner could have insisted on Applicant narrowing the scope of statistical information. However, Yavatkar in fact fails to mention or suggest collecting statistical information, and thus all that Applicant needs to distinguish this feature over Yavatkar is the act of collecting statistical information.

Instead Yavatkar describes gathering information as: "gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process." [Yavatkar Col. 2, line 56]. Yavatkar also discloses: "In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. [Yavatkar Col. 4, line 16].

In *Morris*, the specification lacked any text to guide the Examiner in construing what the disputed claim term meant. Based on the absence of any such text, the Court stated that the Examiner's interpretation was reasonable:

> Absent an express definition in their specification, the fact that appellants can point to definitions or usages that conform to their interpretation does not make the PTO's definition unreasonable when the PTO can point to other sources that support its interpretation."

In the present application, the written description discusses querying data collectors, and statistical information on network packets in great detail. There is no ambiguity, as there was in *Morris*. Nevertheless, the examiner, by construing querying data collectors and collecting statistical with totally unrelated concepts, improperly ignores the meaning that these features

have in Appellant's specification and the meaning given to the terms bloodhound agent and gathering information as disclosed by Yavatkar.

Appellant does not ask the examiner to read limitations into the claims as was the case in *In re Van Geuns*[2]. In *Van Geuns*, the specification disclosed a magnet assembly used for NMR. The claim, however, recited a magnet assembly that provided a uniform magnetic field, with no mention of NMR. The cited reference disclosed a magnet assembly that generated a relatively uniform field. *Van Geuns* is inapplicable to the present case, because the claim elements, e.g., querying data collectors and collecting statistical information are expressly defined in the specification and positively recited in the claims.

Rather, Applicant's claims recite particular features and the Examiner must find those features in the prior art rather than conflate them with totally non-relevant teachings. So the specification is available to the examiner to help her understand what these features mean.

Accordingly, it is well established that the Examiner may properly review the specification in construing a claim term. In the present case, the Examiner is attempting to construe these features without the benefit of the guidance offered by Applicant's specification. In rejecting such guidance, the Examiner has been cast adrift, so much so that she now confuses "querying data collectors" with "launching bloodhound agents" and "collecting statistical information" with "gathering information."

Notwithstanding these distinctions over Yavatkar, claim 1 also requires processing the statistical information to determine the source of suspicious network traffic sent to the data center. The examiner states that: "After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the currently claimed limitations."

However, according to Yavatkar, the bloodhound agents work in a different manner. The bloodhound agents attempt to trace back over links to the source. As explained by Yavatkar, "To

---

[2] *In re Van Geuns*, 988 F.2d 1181 (Fed. Cir. 1993).

trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found."

Thus, unlike claim 1, which requires processing of statistical data on network traffic, Yavatkar launches mobile agents that instantiate themselves to follow links to the source of an attack. Therefore, the examiner's interpretation of Yavatkar is in error and in no sense does Yavatkar describe or suggest claim 1.

Claims 2-12 are distinct over Yavatkar at least for the reasons discussed in claim 1 and for the reasons of record.

Claim 15 is an independent claim that contains analogous features as claim 1. For instance, claim 15 requires sending queries to data collectors ... that ... collect statistical information on network packets sent over the network, the queries being requests for statistical information from data collectors that have examined network traffic with the victim destination address and determining the data center or centers involved in the attack ... by analyzing collected statistical information from the data collectors. As with claim 1, claim 15 requires collecting statistical information, querying data collectors and more explicitly requires determining the ... centers involved in the attack ... by analyzing collected statistical information from the data collectors. Yavatkar does not teach any of these features.

Claims 16-19 are allowable over Yavatkar at least for the reasons discussed in claim 15 and for the reasons of record.

Claim 20 is directed to a system to thwart denial of service attacks on a victim data center. Claim 20 contains analogous limitations as claims 1 and 15 and is allowable for analogous reasons.

Claims 21-33 further distinguish over Yavatkar. For instance, claim 23 requires that the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack. Yavatkar fails to disclose statistical information and thus fails to disclose that the control center and gateway device ... exchange data including

statistical information to thwart the attack. Claim 24 recites that the data exchanged between the control center and gateway device ... are sent over a redundant network that is a different network than the network that is being monitored by the data collectors. Yavatkar fails to disclose a redundant network.

Claims 25 and 26 further distinguish since Yavatkar fails to suggest that ... the control center issues a request to the gateway that the source of the attack is behind to block the attacking traffic or that ... the control center issues a request to the gateway to selectively discard traffic that contains the victim destination address.

Claim 29 serves to distinguish over Yavatkar for analogous reasons as in claim 1 and 15 and claims 30-33 are allowable for analogous reasons.

The examiner rejected Claim 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al., '702 and in view of Hill et al., (Hill) U.S. Pat No. 6,088,804.

Claims 13 and 14 are allowable at least because the base claims are allowable over the references and that Hill does not cure the deficiencies in Yavatkar as noted in the above argument.

Further, the examiner uses Hill to teach "classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2 lines 53-60; col. 6 lines 9-22)." Applicant notes that the teachings in Hill are directed to attack simulation, not to an actual attack.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim

does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

No fee is believed due. If a fee is due please apply that fee and any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 9/1/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21399849.doc